File # 19-009
PPD # 18-0045
Exp date: 2/27/2024

MEMORANDUM OF UNDERSTANDING
between
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT,
HOMELAND SECURITY INVESTIGATIONS, LOS ANGELES
and
THE LOS ANGELES POLICE DEPARTMENT

1. PARTIES

The parties to this Memorandum of Understanding (MOU) are the U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement, Homeland Security Investigations (HSI) Los Angeles, and the Los Angeles Police Department (LAPD).

2. AUTHORITIES

HSI's authority to enter this MOU derives from, among other authorities, the Homeland Security Act of 2002, codified in Title 6 of the United States Code; the HERO Act of 2015, codified at 6 U.S.C. § 473(c); and applicable DHS internal delegation orders.

Nothing in this MOU is intended to conflict with current law, regulation, or policy. Further, nothing in this MOU is intended to restrict the authority of either party to act as provided by law or regulation, or to restrict any agency from enforcing any laws within its authority or jurisdiction. If any term of this MOU is inconsistent with law, regulation, policy, or other authority, then that term shall be invalid, but the remaining terms and conditions of this MOU shall remain in full force and effect.

3. PURPOSE

The purpose of this MOU is to set forth the terms by which the parties will conduct joint computer forensic training and coordination in support of investigations targeting criminal activity. The initiative will enhance cooperation and focus the combined investigative powers, experience and technological expertise of the parties to identify and analyze pertinent digital evidence in criminal investigations.

4. RESPONSIBILITIES

HSI agrees:

A. To provide LAPD a 5-week Basic Computer Evidence Recovery Training (BCERT) course to HSI-approved, LAPD-selected personnel who are assigned to conduct computer forensic investigations as part of at least fifty percent (50%) of their duties. This training prepares investigators to conduct computer and mobile device forensics, and includes concepts such as: write-blocking, hashing, searching,

file systems, virtualization, and use of forensic software (EnCase, Forensic Toolkit and WinHex), data acquisition methods, legal issues related to the field of digital forensics, and mobile device acquisition techniques and technology (Cellebrite Mobile Forensic Software);

B. To supply computer equipment to enable each LAPD student of the BCERT course to conduct computer forensic investigations within HSI-designated workspace. The equipment will be loaned to the LAPD for the course of the investigator's assignment as a computer forensic investigator within LAPD. The equipment may be comprised of a computer forensic desktop, laptop, and search warrant kit to include write-blockers, adapters and computer toolkit(s). However, collocation of LAPD personnel within HSI facilities is not required;

C. To offer annual and reoccurring opportunities for training and collaboration to enhance and otherwise maintain the computer forensic skillsets developed by LAPD personnel;

D. To provide the capability to further criminal investigations with international nexus and which meet federal prosecutorial thresholds; and,

E. To cover the costs associated with any pre-requisite BCERT examinations, at HSI discretion.

LAPD agrees:

A. To provide joint workspace for HSI personnel to assist LAPD with state and local criminal investigations where the criminal conduct involves the use of computer technology;

B. To offer HSI the right of first refusal among other federal agencies for federal adoption of assets seized lawfully by LAPD, whenever the conduct giving rise to the seizure violates federal law and the use of computer technology was a component of the crime, pursuant to the U.S. Attorney General's July 19, 2017 Order on Federal Adoption and Forfeiture of Property Seized by State and Local Law Enforcement Agencies;

C. To offer HSI the right of first refusal among other federal agencies to assume responsibility over LAPD criminal casework, whenever the criminal conduct violates federal law, meets federal thresholds, and the use of computer technology was a component of the crime;

D. That its computer forensic personnel will input into the relevant HSI computer system the specifications of digital devices they encounter and analyze pursuant to LAPD or HSI criminal investigations. However, reporting of the details of the related case or investigation is not required; and,

E. To abide by the terms and polices of Attachment A, attached hereto and incorporated herein, entitled the "Nomination Process for Computer Forensics Training and Use of HSI Equipment." These terms and polices are requirements derived from the HSI Special Agent Handbook. Reference to Special Agents or Computer Forensic Analysts applies to State and Local Agency personnel acting pursuant to this MOU.

5. INDEMNIFICATION AND LEGAL MATTERS

Neither party is required to insure, defend or indemnify the other; rather, the parties agree that they shall remain responsible for any liability arising from their own employees' conduct to the extent and in the manner provided by federal and state law. Additionally, if an HSI employee is injured, he or she would be covered under the provisions of the Federal Employees' Compensation Act, and this liability would not extend to LAPD.

Throughout the course of investigations and enforcement activities, legal advice may be obtained from the assigned prosecutors or participating agency counsel as required by law and policy; however, the parties agree to advise HSI counsel of any court proceeding in which the validity of a Customs Officer's search, seizure or arrest authority becomes an issue, or any potential liability to HSI occurs, and to permit HSI counsel to provide legal memoranda, or other assistance in such cases when desired by HSI.

6. DOCUMENTATION AND DISCLOSURE

HSI and LAPD will maintain their own records and reports relating to their own casework. Furthermore, the LAPD agrees to coordinate with HSI prior to releasing any information relating to or exchanged under this MOU. Information obtained or developed because of this MOU—including but not limited to evidence, byproducts of evidence, methodologies, standard operating procedures, training materials provided, and forensic software utilized—is under the control of HSI and shall be subject to public disclosure only pursuant to the provisions of federal laws, regulations, and executive orders, including pursuant to the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a.

Notwithstanding the foregoing, and anything to the contrary in this MOU, records owned, used, possessed, or maintained by LAPD are subject to public disclosure pursuant to the provisions of the California Public Records Act (CPRA), California Government Code section 6250, *et seq*. Moreover, nothing in this MOU is intended to or shall prevent LAPD from fulfilling its legal obligations under the CPRA or any other law, regulation, or court order.

7. PRE-REQUISITE FOR BASIC COMPUTER EVIDENCE RECOVERY TRAINING

To be considered for enrollment in the BCERT course, the personnel selected by LAPD must be able to obtain a CompTIA A+ certification, on their own, and at least 3 months prior to the first day of the training course. A CompTIA A+ certification exam, an industry standard equivalent exam, or other exam, as designated by HSI, must be completed at a satisfactory level by the nominee. HSI will cover the costs associated with any required examination, at HSI discretion. Additionally, the individual selected by LAPD must agree to perform computer forensics as part of LAPD assigned duties for a minimum of 3 years, following completion of the BCERT course. The LAPD agrees to support this 3-year commitment unless extraordinary circumstances prevent it. These requirements do not preclude LAPD personnel from promotion or other advancements.

8. INTERNAL INVESTIGATIONS/MISCONDUCT/CRITICAL INCIDENTS

All complaints, allegations, or information relative to misconduct or breaches of integrity involving HSI or LAPD personnel, will be investigated in accordance with the rules and guidelines of the accused individual's employing agency. HSI and LAPD agree to cooperate with internal affairs or professional conduct/responsibility investigators of participating agencies in accordance with the policy of the accused individual's employing agency.

9. ASSET SHARING

Whenever possible, the parties agree to engage in equitable sharing of forfeited assets to the extent permissible in accordance with the laws, regulations, policies, and bylaws applicable to each party. HSI shall be responsible for the processing of forfeitures of assets seized for federal forfeiture in conjunction with applicable LAPD operations; when the seizure was made with sufficient direct, pre-seizure involvement by an assigned HSI Special Agent or at the time of the seizure, the seizing officer was acting under the direction of, or in real-time, hand-in-hand cooperation with an HSI Special Agent or the seizure made as part of a pre-existing federal or joint federal-state investigation in which the assigned HSI Special Agent was pursuing federal criminal charges.

Under the U.S. Attorney General's July 19, 2017 Order on Federal Adoption and Forfeiture of Property Seized by State and Local Law Enforcement Agencies, federal adoption of all types of assets seized lawfully by state or local law enforcement under their respective state laws is authorized whenever the conduct giving rise to the seizure violates federal law, applying the factors outlined in the U.S. Department of Justice's (DOJ) Policy Directive 17-1, "Policy Guidance on the Attorney General's Order on Federal Adoption and Forfeiture of Property Seized by State and Local Law Enforcement Agencies" (July 19, 2017). To adopt a seizure will be at the sole determination of the Federal Government, pursuant to applicable law and policy, including DOJ, Department of Treasury, and DHS policies.

10. PRESS RELEASES

The LAPD agrees to coordinate with HSI in advance of any release of information to the media relating to the joint activities of the parties. Media releases shall not include information regarding confidential investigative sources, techniques, privileged information, or information protected from disclosure by law or policy.

11. DECONFLICTION

The parties agree that the deconfliction process requires the sharing of certain operational information, which, if disclosed to unauthorized persons, could endanger law enforcement personnel and the public. LAPD agrees to coordinate with HSI prior to releasing any information obtained or developed under this MOU. The parties agree to adopt reasonable security measures, including safeguarding passwords, codes, equipment, and evidence. The parties also agree to assign primary points of contact for matters relating to this MOU. The parties will update each other anytime a point of contact changes.

12. MODIFICATION

The terms of this MOU may be modified by the signed, written agreement of both parties.

13. TERMINATION

Either party may unilaterally terminate this MOU upon 30-days written notice to the other. The parties agree that if a party exercises this right of unilateral termination, it shall, to the extent practicable, do so in a manner as to minimize any adverse impact on the other party. Each party will make best efforts to act in good faith to continue the MOU.

14. PARTICIPATION SUBJECT TO FUNDING

The parties' participation in this agreement is subject to their respective budgeting processes. HSI's participation is subject to the availability of appropriated funding. This MOU does not in itself constitute an obligation of funds.

15. CIVIL IMMIGRATION ENFORCEMENT

The parties agree that LAPD personnel shall comply with LAPD policies and procedures regarding immigration enforcement during their participation in any task force activity.

The parties further agree that LAPD personnel shall not participate in, nor assist with, civil immigration enforcement, and if deputized as a federal task force officer, LAPD personnel will not accept any legal authority to enforce civil immigration offences.

16. EFFECTIVE DATE

This MOU shall become effective as of the date it is signed by both parties and shall remain in effect for one year and automatically renewed up to five-years if the agreement has not been modified or terminated in the manner set forth above.

17. POINTS OF CONTACT

The points of contact and recipient for all required notices shall be the following:

A. HSI
Garrick B. Carlton
Deputy Special Agent in Charge
501 West Ocean Blvd., Suite 7200
Long Beach, California 90802
Office: (562) 624-3808; Cell: [redacted]

B. LAPD
Lieutenant Andrea Grossman
LA Regional ICAC Commander
501 West Ocean Blvd., Suite 7200
Long Beach, California 90802
Office: (562) 624-4027; Cell: [redacted]

18. NO PRIVATE RIGHT CREATED

This MOU is an internal MOU and does not create or confer any right or benefit on any other person or party, private or public.

19. SIGNATORIES

This MOU is agreed to by the signatures of the duly authorized officials of the parties as set forth below, who warrant that they are authorized to bind their respective agency to this MOU.

SIGNED AND AGREED UPON:

Homeland Security Investigations, Los Angeles

JOSEPH MACIAS, Special Agent in Charge

Date: 2/27/2019

Los Angeles Police Department

MICHEL R. MOORE, Chief of Police

Date:

19. SIGNATORIES

This MOU is agreed to by the signatures of the duly authorized officials of the parties as set forth below, who warrant that they are authorized to bind their respective agency to this MOU.

SIGNED AND AGREED UPON:

Homeland Security Investigations, Los Angeles

JOSEPH MACIAS, Special Agent in Charge — Date:

Los Angeles Police Department

MICHEL R. MOORE, Chief of Police — Date: 8-1-18

ATTACHMENT "A" to MOU Between HSI and LAPD

NOMINATION PROCESS FOR COMPUTER FORENSICS TRAINING AND USE OF HSI EQUIPMENT

Nomination Process for Computer Forensics Program Training

Based upon workload, HSI will determine the number of candidates nominated by LAPD. LAPD will submit the following information for each candidate:

A. Name;

B. Contact information;

C. State and Local Agency;

D. State and Local Agency office location, actual workspace of nominee;

E. Candidate's entrance on duty date;

F. Brief biography of the candidate's computer knowledge and experience;

G. Acknowledgement of three year mandatory term of service;

H. Acknowledgement of one year probationary period;

I. Need for a Computer Forensics Analyst (CFA) or an additional CFA for a specific office location;

J. Request for training; and

K. If applicable, substantiated Giglio and/or Henthorn issues and/or a list of any disciplinary actions of record that might raise Giglio and/or Henthorn issues, or letters from the District Attorney and/or U.S. Attorney's Offices regarding such issues.

Mentorship

A mentor is a CFA who has already acquired a CompTIA A+ Certification, and successfully attended the Basic Computer Evidence Recovery Training (BCERT) course issued by HSI or equivalent. The mentor will normally be selected from within the same office as that of the probationary CFA. If the probationary CFA is the only CFA in the office, the mentor CFA will be selected from within the HSI Los Angeles Area of Responsibility (AOR). If there is no

qualified mentor CFA in the designated AOR, a mentor CFA in another AOR or in the Cyber Crime Center (C3) will be selected.

The mentor CFA will review reports and examinations for format and presentation prior to their submission. The mentor CFA will also be available to answer questions the CFA may have during the course of the examinations. When possible, the mentor CFA should observe the probationary CFA's first few examinations. If the mentor CFA is not located in the same office as the probationary CFA, the probationary CFA should provide to the mentor CFA copies of any completed work product and associated files that he or she produces during the mentoring process.

Equipment and Software

All equipment issued to the law enforcement officer (LEO) or the task force officer (TFO) remains the property of HSI and may be utilized only in a manner consistent within LAPD policy and procedures which pertain to the integrity of digital evidence. A set of approved analysis programs will be supplied to all CFAs during the basic, advanced, or specialized training classes. These programs have been approved by the HSI Computer Forensics Unit (CFU). The most current list of approved analysis software is maintained by the CFU.

The requirement to use "approved software" does not refer to programs that are used to "preview" or "triage" contents of media devices. This also does not include tools needed for more specialized tasks, such as index.dat viewers, outside image viewers, *.pst viewers, or media viewers.

Programs that do not appear on the approved software list cannot be used by CFAs without prior approval by CFU. Any software program that does not fall into one of the above categories is considered supplemental software. These program types include, but are not limited to, viewers, media players, and other specialized software. Any software that has not been issued by CFU, or does not appear on the approved software list, cannot be utilized by CFAs without prior notification and approval by CFU. A list of approved supplemental programs will be provided to each CFA and updated within the CFU FTP site. In certain situations, it may be necessary for CFAs to use a unique supplemental software program pursuant to an exigent circumstance. In those situations, CFAs should ensure that the program performs as stated by the developer. In addition, CFAs should notify CFU as soon as possible after utilizing the software.

With the exception of hardware that is not an imaging or write blocking hardware, all new write blocking or imaging hardware and all software that is not on any of the approved lists or has not been tested by National Institute of Standards and Technology (NIST) must be approved by CFU. CFU will make the determination as to whether the write blocking hardware, imaging hardware, or software will be purchased or not. If the tool has already been purchased, it cannot be utilized by CFAs until it has been tested and validated by the Computer Forensics Program (CFP). Any hardware or software that has been tested and verified by NIST can be used by CFAs without CFU approval.

CFAs must first contact CFU via e-mail to start the approval procedures. The e-mail must contain the name of the tool, manufacturer, anticipated use, and cost. (Note: Approval for hardware such as hard drives, motherboards, and expansion cards is not required.) The approval procedures for use of new write blocking hardware, imaging hardware, or software require that a suitable number of CFAs must determine, through testing, that the write blocking hardware, imaging hardware, or software performs as expected. CFAs will report their findings to CFU which will make the final determination as to the use of the write blocking hardware, imaging hardware, or software in the CFP.

Removal from the Computer Forensics Program During the Probationary Period in the Program

During a new CFA's probationary period in the CFP, the CFA may be removed from the CFP by the CFU Unit Chief based on CFP needs or if the CFA does not meet the requirements specified in this memorandum.

If the mentor CFA, or any active CFA, or supervisor determines that the probationary CFA is unable to complete examinations accurately and/or in a timely fashion, or that the probationary CFA lacks the base level of knowledge required, the mentor CFA or an, active CFA, or supervisor can request that the CFU Unit Chief and/or LAPD conduct a secondary review of the probationary CFA's work product. If the CFU Unit Chief determines that the work product does not meet the standards of the program, he or she can remove the CFA from the CFP.

Upon removal, the CFA's equipment will be reacquired and reassigned by CFU. CFAs can be removed from the CFP for prolonged inactivity, failure to complete assignments or training, or any performance issues as CFAs, as determined by the CFU Unit Chief. The CFU Unit Chief will make the final decision as to the permanent status of the CFA.

Removal from the Computer Forensics Program During the Initial 3-Year Term of Service in the Program

CFAs are required to remain in the CFP during their initial 3-year term of service. However, LAPD may remove a CFA from his or her duties as a CFA during the initial 3-year term of service. LAPD may accomplish this by obtaining, via memorandum, the concurrence of the HSI CFU Unit Chief. The memorandum should include the reasons for LAPD's intention to remove the CFA from his or her binding agreement.

The CFU Unit Chief may remove the CFA from the CFP for any reason.

Removal from the Computer Forensics Program After the Initial 3-Year Term of Service in the Program

After the initial commitment is fulfilled, LAPD may remove the CFA from his or her responsibilities as a CFA for any reason. A memorandum to the CFU Unit Chief is required six (6) months prior to the CFA's removal from the CFP, and must include the reasons for the

removal. Due to the amount of time and money invested in the training of the CFAs, there must be specific, documented cause to remove someone from the program.

After the initial commitment is fulfilled, CFAs may remove themselves from the CFP for any reason. The CFA must route a memorandum of intent to the CFU Unit Chief, through LAPD, at least six (6) months prior to his or her removal from the CFP. This six-month period is intended to provide the CFU Unit Chief and the LAPD appropriate time to make arrangements for a possible replacement.

Notification of Change of Computer Forensics Agent/Computer Forensics Analyst Status and Return of Computer Forensics Unit Equipment

Upon a CFA's separation from service, retirement, or termination of active CFA status, LAPD must notify the CFU Unit Chief. The CFU Unit Chief will determine the final disposition of all issued computer forensics equipment.